

---

## **Nortel Communication Server 1000**

Nortel Networks Communication Server 1000 Release 4.5

---

# **WLAN Handset 2212**

## **Installation and Configuration for VPN**

Document Number: 553-3001-229

Document Release: Standard 1.00

Date: November 2005

---

Copyright © Nortel Networks Limited 2005

All Rights Reserved

Produced in Canada

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

Nortel, Nortel (Logo), the Globemark, This is the Way, This is Nortel (Design mark), SL-1, Meridian 1, and Succession are trademarks of Nortel Networks.

---



## Revision history

---

### November 2005

Standard 1.00. This document is a new NTP issued to support Communication Server 1000 Release 4.5.



---

# Contents

---

|                                      |           |
|--------------------------------------|-----------|
| <b>List of procedures</b>            | <b>7</b>  |
| <b>How to get help</b>               | <b>9</b>  |
| <b>About this document</b>           | <b>11</b> |
| Subject                              | 11        |
| Applicable systems                   | 11        |
| Intended audience                    | 13        |
| Conventions                          | 13        |
| Related information                  | 14        |
| <b>Overview</b>                      | <b>15</b> |
| Contents                             | 15        |
| Introduction                         | 15        |
| Code and key code requirements       | 16        |
| Scope of this document               | 16        |
| <b>Getting started</b>               | <b>19</b> |
| Contents                             | 19        |
| Introduction                         | 19        |
| Configuring the Contivity VPN router | 19        |
| Installing the Licence Keys          | 26        |
| <b>DHCP options</b>                  | <b>29</b> |
| Contents                             | 29        |

|                                                          |           |
|----------------------------------------------------------|-----------|
| Introduction .....                                       | 29        |
| The DHCP server .....                                    | 29        |
| Checking connectivity .....                              | 30        |
| DHCP relay .....                                         | 31        |
| <b>IP address pool configuration .....</b>               | <b>33</b> |
| Contents .....                                           | 33        |
| Introduction .....                                       | 33        |
| IP address pools .....                                   | 33        |
| Proxy ARP and tunnel-to-tunnel traffic .....             | 35        |
| <b>IPsec options and groups .....</b>                    | <b>37</b> |
| Contents .....                                           | 37        |
| Introduction .....                                       | 37        |
| IPsec global variables .....                             | 37        |
| WLAN Handset 2212 group definition .....                 | 39        |
| WLAN Handset 2212 group IPsec variables .....            | 40        |
| <b>Users, interface and firewall configuration .....</b> | <b>45</b> |
| Contents .....                                           | 45        |
| Introduction .....                                       | 45        |
| User accounts .....                                      | 45        |
| Second interface configuration .....                     | 48        |
| Firewall configuration .....                             | 52        |
| <b>Handset configuration .....</b>                       | <b>57</b> |
| Contents .....                                           | 57        |
| Introduction .....                                       | 57        |
| Configuring the handset .....                            | 57        |

---

# List of procedures

---

|                                                             |    |
|-------------------------------------------------------------|----|
| Procedure 1                                                 |    |
| Configuring the VPN router .....                            | 19 |
| Procedure 2                                                 |    |
| Installing licence keys .....                               | 26 |
| Procedure 3                                                 |    |
| Disabling the DHCP server .....                             | 29 |
| Procedure 4                                                 |    |
| Enabling the DHCP relay .....                               | 31 |
| Procedure 5                                                 |    |
| Configuring an IP address pool .....                        | 33 |
| Procedure 6                                                 |    |
| Enabling proxy ARP and tunnel-to-tunnel traffic .....       | 35 |
| Procedure 7                                                 |    |
| Setting IPsec global variables .....                        | 37 |
| Procedure 8                                                 |    |
| Defining a WLAN Handset 2212 group .....                    | 39 |
| Procedure 9                                                 |    |
| Setting IPsec variables for a WLAN Handset 2212 group ..... | 40 |
| Procedure 10                                                |    |
| Adding a user account .....                                 | 45 |

**Procedure 11**  
**Configuring the second interface .....48**

**Procedure 12**  
**Configuring the firewall .....52**

**Procedure 13**  
**Configuring the WLAN Handset 2212 using the**  
**cradle .....58**

**Procedure 14**  
**Configuring the WLAN Handset 2212 using the**  
**screen .....59**

# How to get help

---

This section explains how to get help for Nortel products and services.

## Getting Help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

[www.nortel.com/support](http://www.nortel.com/support)

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

## Getting Help over the phone from a Nortel Solutions Center

If you don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

[www.nortel.com/callus](http://www.nortel.com/callus)

## **Getting Help from a specialist by using an Express Routing Code**

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

[www.nortel.com/erc](http://www.nortel.com/erc)

## **Getting Help through a Nortel distributor or reseller**

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

## About this document

---

This document is a global document. Contact your system supplier or your Nortel representative to verify that the hardware and software described are supported in your area.

### Subject

This document describes the installation and configuration of a WLAN Handset 2212 on a Virtual Private Network.

#### **Note on legacy products and releases**

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 4.5 software. For more information on legacy products and releases, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

[www.nortel.com](http://www.nortel.com)

### Applicable systems

This document applies to the following systems:

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M Chassis (CS 1000M CH)
- Communication Server 1000M Cabinet (CS 1000M CA)
- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)

- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

**Note:** When upgrading software, memory upgrades may be required on the Signaling Server, the Call Server, or both.

### System migration

When particular Meridian 1 systems are upgraded to run CS 1000 Release 4.5 software and configured to include a Signaling Server, they become CS 1000M systems. Table 1 lists each Meridian 1 system that supports an upgrade path to a CS 1000M system.

**Table 1**  
**Meridian 1 systems to CS 1000M systems**

| This Meridian 1 system... | Maps to this CS 1000M system |
|---------------------------|------------------------------|
| Meridian 1 PBX 11C CH     | CS 1000M CH                  |
| Meridian 1 PBX 11C CA     | CS 1000M CA                  |
| Meridian 1 PBX 51C        | CS 1000M Half Group          |
| Meridian 1 PBX 61C        | CS 1000M Single Group        |
| Meridian 1 PBX 81         | CS 1000M Multi Group         |
| Meridian 1 PBX 81C        | CS 1000M Multi Group         |

For more information, see one or more of the following NTPs:

- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures* (553-3011-258)

- *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures (553-3021-258)*
- *Communication Server 1000S: Upgrade Procedures (553-3031-258)*
- *Communication Server 1000E: Upgrade Procedures (553-3041-258)*

## Intended audience

This document is intended for individuals responsible for installing, configuring, operating, and maintaining the WLAN Handset 2212.

## Conventions

### Terminology

In this document, the following systems are referred to generically as “system”:

- Communication Server 1000M (CS 1000M)
- Communication Server 1000E (CS 1000E)
- Communication Server 1000S (CS 1000S)
- Meridian 1

The following systems are referred to generically as “Small System”:

- Communication Server 1000M Chassis (CS 1000M CH)
- Communication Server 1000M Cabinet (CS 1000M CA)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet

The following systems are referred to generically as “Large System”:

- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Meridian 1 PBX 51C

- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

## Related information

This section lists information sources that relate to this document.

### Online

To access Nortel documentation online, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

[www.nortel.com](http://www.nortel.com)

### CD-ROM

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

---

# Overview

---

## Contents

This section contains information on the following topics:

|                                              |    |
|----------------------------------------------|----|
| Introduction . . . . .                       | 15 |
| Code and key code requirements . . . . .     | 16 |
| Scope of this document . . . . .             | 16 |
| Assumptions . . . . .                        | 16 |
| The configuration in this document . . . . . | 17 |

## Introduction

The WLAN Handset 2212 is a mobile handset for workplace IP telephone systems. The handset operates over an 802.11b wireless Ethernet LAN providing users a wireless Voice Over IP (VoIP) extension. By seamlessly integrating with the Nortel IP telephony system, handset users are provided with high-quality mobile voice communications throughout the workplace. The handset gives users the freedom to roam throughout the workplace while providing all the features and functionality of an IP desk telephone.

The WLAN Handset 2212 provides a wireless extension to the Nortel Meridian 1 and CS 1000 VoIP solutions. The handset supports the UNISTim protocol, a proprietary protocol developed by Nortel for communication between a Nortel IP telephone and a Nortel PBX.

The handsets reside on the wireless LAN with other wireless devices using Direct Sequence Spread Spectrum (DSSS) radio technology. The handset radio transmits and receives packets at up to 11Mb/s.

**IMPORTANT!**

The latest software version is required to support the features described in this document.

**Code and key code requirements**

Before configuring the WLAN Handset 2212, you must ensure the various components are using the proper versions of software. Table 2 lists the components and software versions:

**Table 2**  
**Required components and software versions**

| Component                      | Software Version                   |
|--------------------------------|------------------------------------|
| WLAN Handset 2212              | 097.060                            |
| WLAN IP Telephony Manager 2245 | 17x.022                            |
| Contivity VPN Router           | V04_90.301                         |
|                                | router can be any model            |
|                                | requires Firewall licence key code |
| CS 1000 or Meridian 1 PBX      | CS 1000 Release 4.0 or higher      |

**Scope of this document**

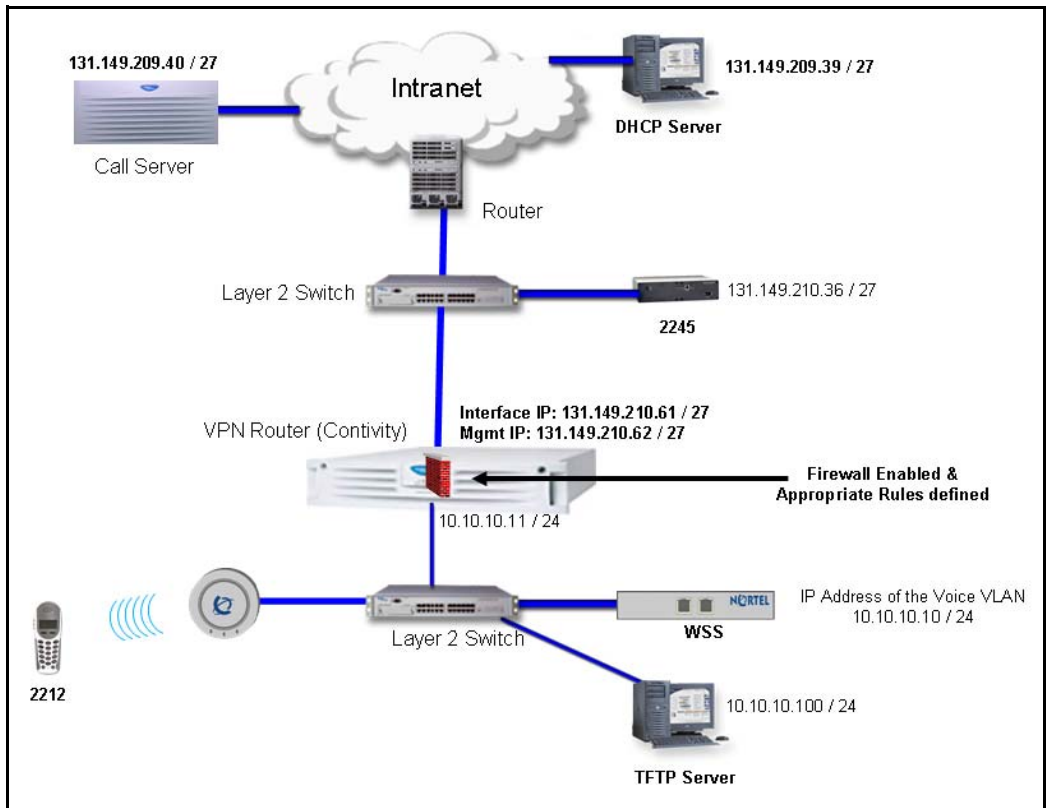
**Assumptions**

- The following assumptions are made in this document:
- The wireless infrastructure has been configured and is available.
  - The PBX has been configured.
  - The WLAN IP Telephony Manager 2245 has been configured.
  - The DHCP server has been programmed and configured to provide the correct IP address.

## The configuration in this document

This document describes the configuration of the supported architecture shown in Figure 1.

**Figure 1**  
**Thin AP – L2 Away from VPN Router**



**IMPORTANT!**

The figures in this document are examples of the types and format of the information required for a specific step. Substitute information for your site accordingly.

---

# Getting started

---

## Contents

This section contains information on the following topics:

|                                                                |                    |
|----------------------------------------------------------------|--------------------|
| <a href="#">Introduction . . . . .</a>                         | <a href="#">19</a> |
| <a href="#">Configuring the Contivity VPN router . . . . .</a> | <a href="#">19</a> |
| <a href="#">Installing the Licence Keys . . . . .</a>          | <a href="#">26</a> |

## Introduction

This section describes how to install and configure the WLAN Handset 2212 for Virtual Private Network (VPN).

## Configuring the Contivity VPN router

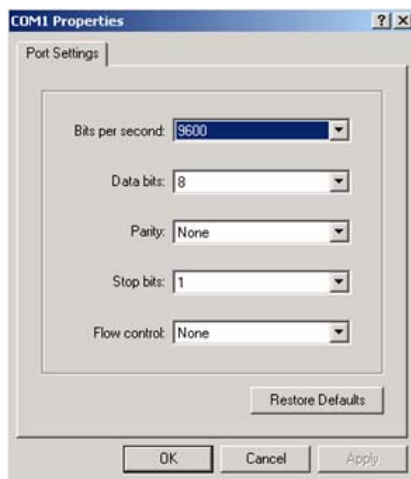
After attaching the console to your PC, use Procedure 1 to configure the VPN router.

### **Procedure 1** **Configuring the VPN router**

- 1** Select **Start > Control Panel**.
- 2** Double click on **System**.  
The System Properties window appears.
- 3** Select the **Hardware** tab.
- 4** Click **Device Manager**.  
The Device Manager window appears.

- 5 Click on the **+** beside **Ports**.  
The Ports list expands.
- 6 Right click **Communications Ports (COM 1)** and select **Properties**.  
The Communications Ports (COM 1) Properties window appears.
- 7 Select the **Port Settings** tab.
- 8 Ensure the settings are configured as shown in Figure 2.

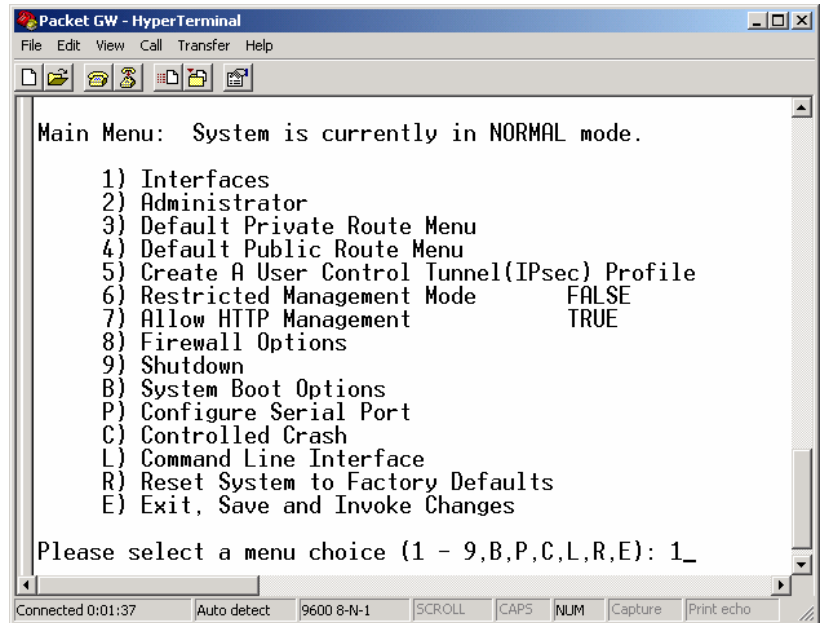
**Figure 2**  
**COM1 settings**



- 9 Connect to the wireless gateway through the console cable.
- 10 Access the wireless gateway using Hyper Terminal.
- 11 Enter the username and password in the **Contivity 1050 Hyper Terminal** window.

The Main Menu window appears, as shown in Figure 3 on [page 21](#)

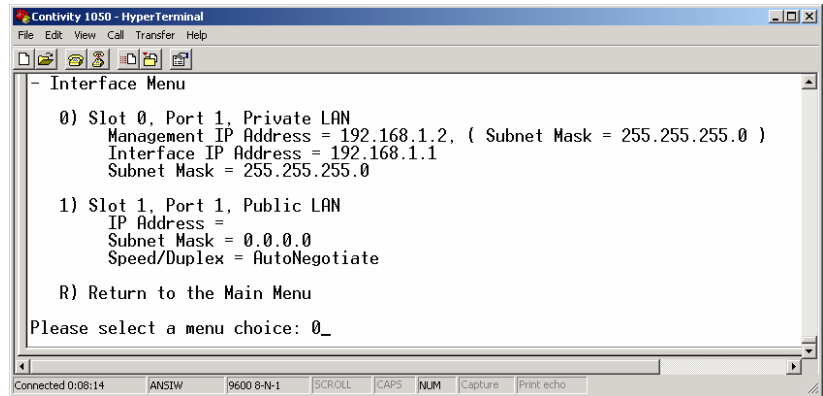
**Figure 3**  
**Main Menu**



**12** Enter 1.

The Interface Menu window appears, as shown in Figure 4 on [page 22](#)

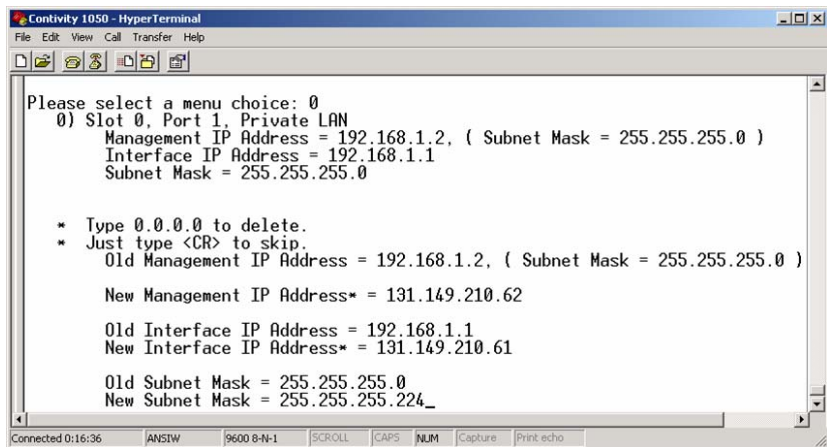
**Figure 4**  
**Interface menu**



**13** Enter 0.

The Private - Trusted Interface window appears, as shown in Figure 5

**Figure 5**  
**Private - Trusted Interface**



**14** Enter the following:

**a. Management IP Address**

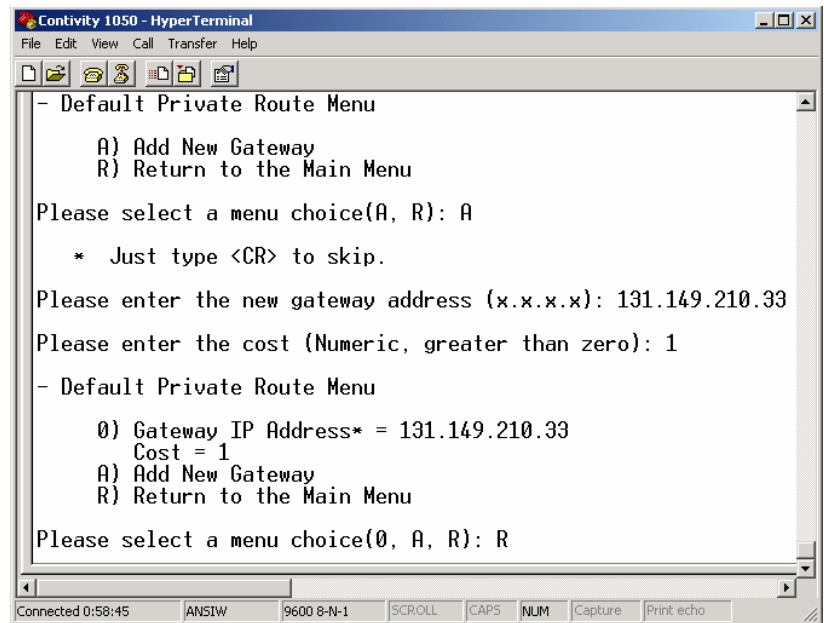
**b. Interface IP Address****c. Subnet Mask**

15 Enter **R** to go back to the **Main Menu**.

16 Enter **3**.

The Default Private Route Menu appears, as shown in Figure 6

**Figure 6**  
**Default Private Route Menu**



17 Enter **A**.

18 Enter a static route to point all the traffic to the default gateway in the **Please enter the new gateway address** field.

19 Enter a cost in the **Please enter the cost** field.

The default value is 1.

20 Enter **R** to return to the **Main Menu**.

21 Enter **E** to exit and save the configuration.

**22** Check the connectivity.

- a.** Log back into your system.
- b.** Open a command line window.
- c.** Ping the gateway.

If you are able to ping the gateway, the VPN router is configured properly.

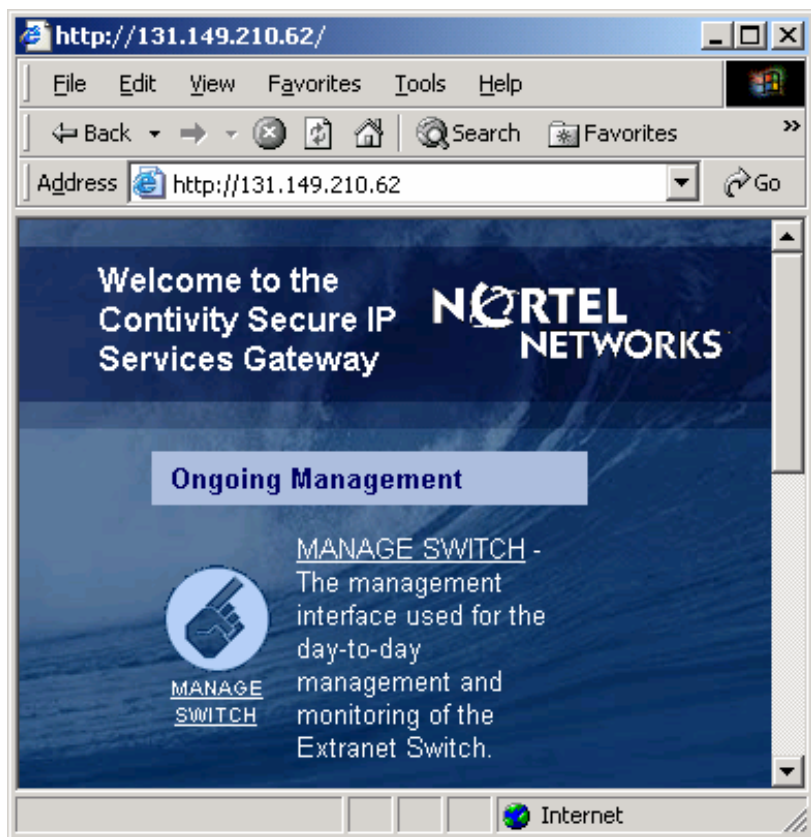
**23** Open Microsoft Internet Explorer.

**24** Enter the Management IP address of the VPN router in the Address bar.

**25** Click **Manage Switch**.

The IP Services Gateway home page appears, as shown in Figure 7 on [page 25](#).

**Figure 7**  
**IP Services Gateway home page**



**26** Enter your login and password.

You can now carry out any required administrative duties.

---

**End of Procedure**

---

## Installing the Licence Keys

Use Procedure 2 to install licence keys.

### IMPORTANT!

The Contivity Stateful Firewall key must be installed for the solution to work.

#### Procedure 2 Installing licence keys

- 1 In the Contivity Secure IP Services Gateway navigator, select **ADMIN > Licence Keys**.
- 2 The Key Installation window appears, as shown in Figure 8.

**Figure 8**  
**Key Installation**

The screenshot shows the 'Key Installation' window in the Contivity Secure IP Services Gateway. The window has a menu bar (File, Edit, View, Favorites, Tools, Help) and a toolbar with navigation icons. The address bar shows 'http://131.149.210.62/manage/topman.htm'. On the left is a sidebar with a tree view containing: SYSTEM, SERVICES, ROUTING, QOS, PROFILES, SERVERS, ADMIN, Administrator, License Keys, Auto Backup, Tools, Recovery, Upgrades, Configs, File System, SNMP, SNMP Traps, and Shutdown. The main area is titled 'Key Installation' and contains a table with three columns: Feature, Key / Status, and Action.

| Feature                     | Key / Status            | Action |
|-----------------------------|-------------------------|--------|
| Advanced Routing            | <input type="text"/>    |        |
| Contivity Stateful Firewall | FW-xxxxxxxxxxxxxxxxxxxx |        |
| VPN Tunnels                 | <input type="text"/>    |        |

At the bottom of the table are 'OK' and 'Cancel' buttons.

- 3 Enter the licence keys in the appropriate fields.

**4** Click **OK**.

---

**End of Procedure**

---



---

# DHCP options

---

## Contents

This section contains information on the following topics:

|                                                 |    |
|-------------------------------------------------|----|
| <a href="#">Introduction</a> . . . . .          | 29 |
| <a href="#">The DHCP server</a> . . . . .       | 29 |
| <a href="#">Checking connectivity</a> . . . . . | 30 |
| <a href="#">DHCP relay</a> . . . . .            | 31 |

## Introduction

This section describes how to set the DHCP options.

## The DHCP server

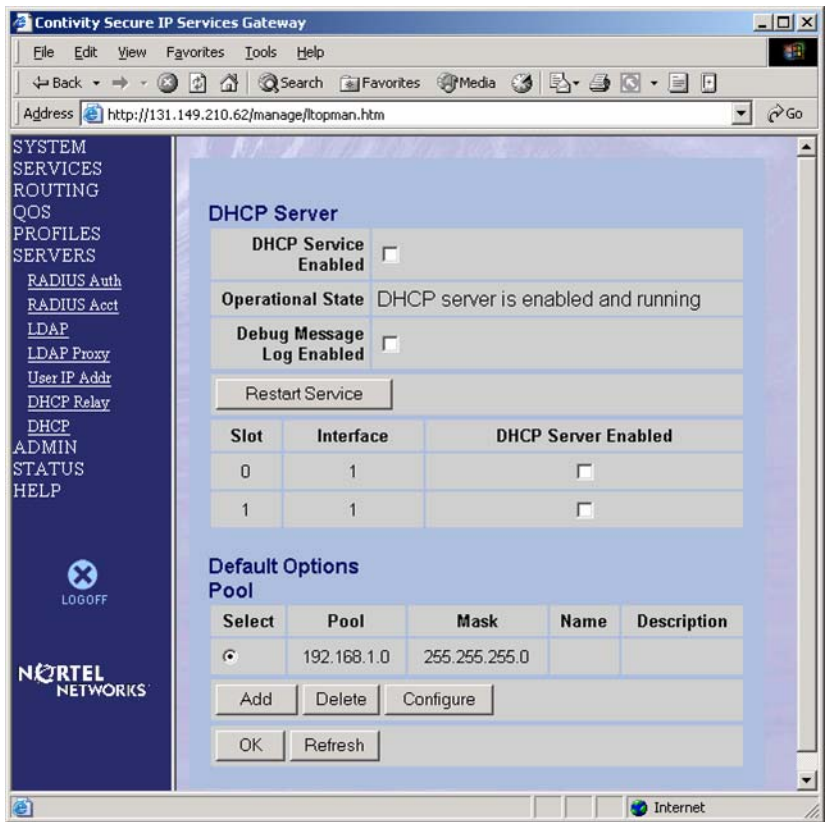
Depending on the model of the VPN router, the DHCP server may already be disabled. Use Procedure 3 to disable the DHCP Server if necessary.

### Procedure 3 Disabling the DHCP server

- 1 In the Contivity Secure IP Services Gateway navigator, select **SERVERS > DHCP**.

The DHCP Servers window appears, as shown in Figure 9 on [page 30](#).

**Figure 9**  
**DHCP Server options**



- 2 Clear the **DHCP Enabled Server** check box.
- 3 Click **OK**.

**End of Procedure**

## Checking connectivity

Test the connectivity for possible routing errors. Open the Console port and ping the DHCP Server, WLAN Application Gateway 2246 and the PBX.

## DHCP relay

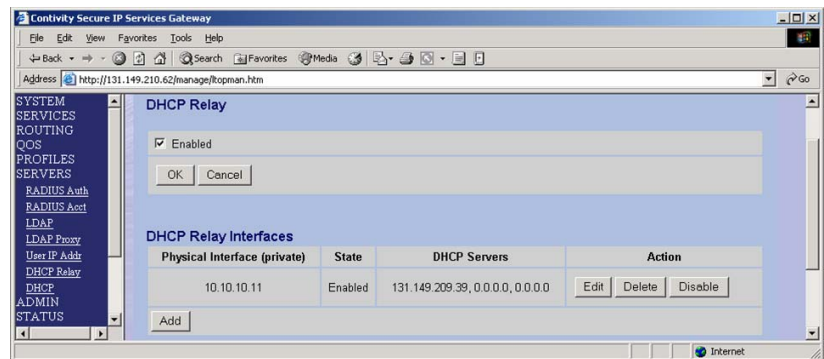
Use Procedure 4 to enable the DHCP Relay.

### Procedure 4 Enabling the DHCP relay

- 1 In the Contivity Secure IP Services Gateway navigator, select **SERVERS > DHCP Relay**.

The DHCP Relay Options window appears, as shown in Figure 10.

**Figure 10**  
**DHCP Relay options**



- 2 Select **Enabled**.

**Note:** Ensure that you add appropriate routes in your network so that the DHCP response from the DHCP server reaches the VPN router.

- 3 Click **OK**.

---

**End of Procedure**

---



---

# IP address pool configuration

---

## Contents

This section contains information on the following topics:

|                                                                  |    |
|------------------------------------------------------------------|----|
| <a href="#">Introduction</a> . . . . .                           | 33 |
| <a href="#">IP address pools</a> . . . . .                       | 33 |
| <a href="#">Proxy ARP and tunnel-to-tunnel traffic</a> . . . . . | 35 |

## Introduction

This section describes how to configure an IP address pool and enable proxy ARP and tunnel-to-tunnel traffic.

## IP address pools

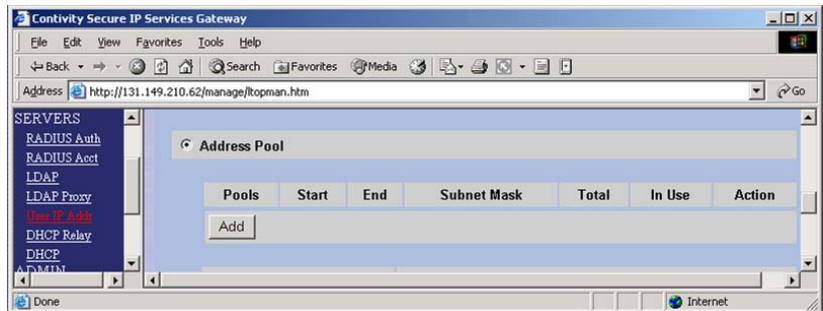
Use Procedure 5 to configure an IP address pool.

### Procedure 5 Configuring an IP address pool

- 1 In the Contivity Secure IP Services Gateway window, select **SERVERS > User IPAddr**.

The User IPAddr window appears, as shown in Figure 11 on [page 34](#).

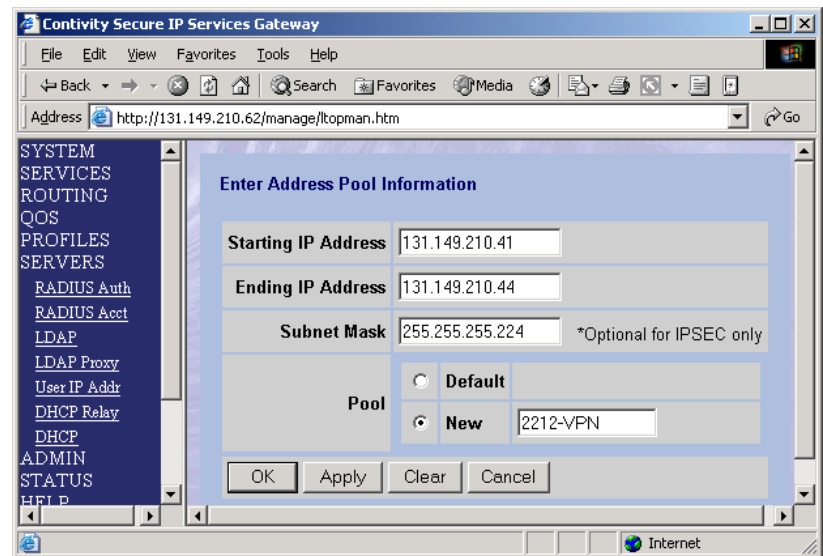
**Figure 11**  
**Add an IP address pool**



2 Click **Add**.

The Address Pool Information window appears, as shown in Figure 12.

**Figure 12**  
**Address pool details**



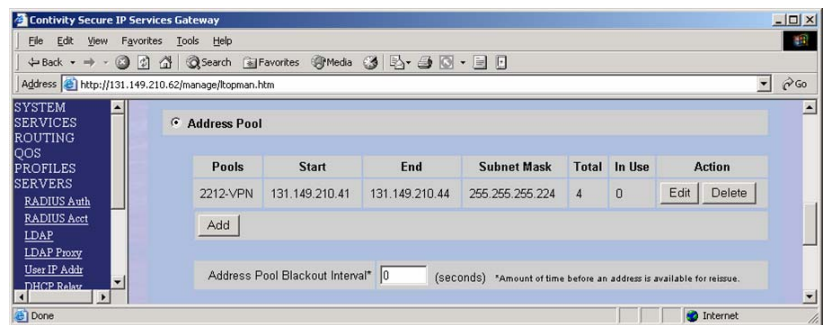
3 Enter a **Starting IP Address**.

4 Enter an **Ending IP Address**.

- 5 Enter a **Subnet Mask**.
- 6 Select **New**.
- 7 Enter a name for the new pool in the text box.
- 8 Click **Apply** to save the details.
- 9 Click **OK**.

The User IPAddr window appears, as shown in Figure 13.

**Figure 13**  
**Address pool**



## Proxy ARP and tunnel-to-tunnel traffic

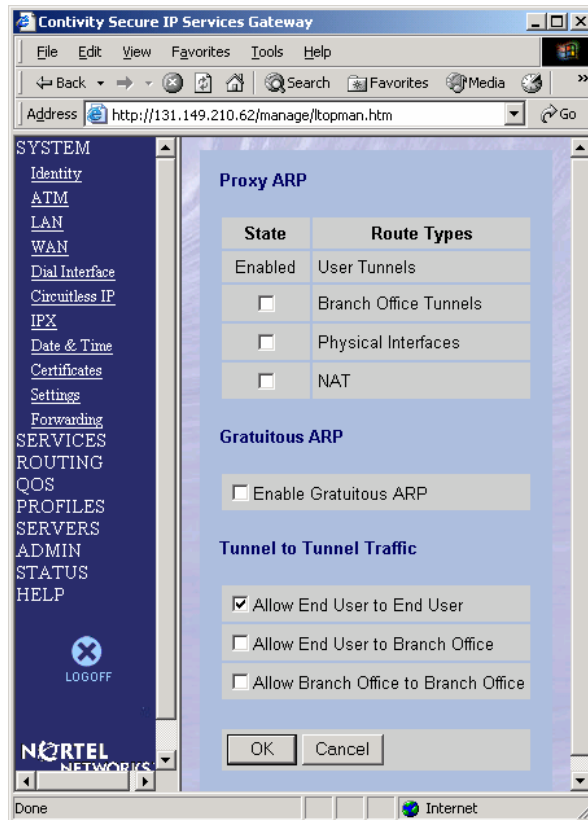
Use Procedure 6 to enable proxy ARP and tunnel-to-tunnel traffic.

### Procedure 6 Enabling proxy ARP and tunnel-to-tunnel traffic

- 1 In the Contivity Secure IP Services Gateway navigator, select **SYSTEM > Forwarding**.

The Forwarding window appears, as shown in Figure 14 on [page 36](#)

**Figure 14**  
**Forwarding options**



- 2 In the **Proxy ARP** section, select the route type you want to enable.
- 3 Select **Allow End User to End User**.
- 4 Click **OK**.

---

**End of Procedure**

---

---

# IPsec options and groups

---

## Contents

This section contains information on the following topics:

|                                                                   |                    |
|-------------------------------------------------------------------|--------------------|
| <a href="#">Introduction . . . . .</a>                            | <a href="#">37</a> |
| <a href="#">IPsec global variables . . . . .</a>                  | <a href="#">37</a> |
| <a href="#">WLAN Handset 2212 group definition . . . . .</a>      | <a href="#">39</a> |
| <a href="#">WLAN Handset 2212 group IPsec variables . . . . .</a> | <a href="#">40</a> |

## Introduction

This section describes how to work with IPsec details.

## IPsec global variables

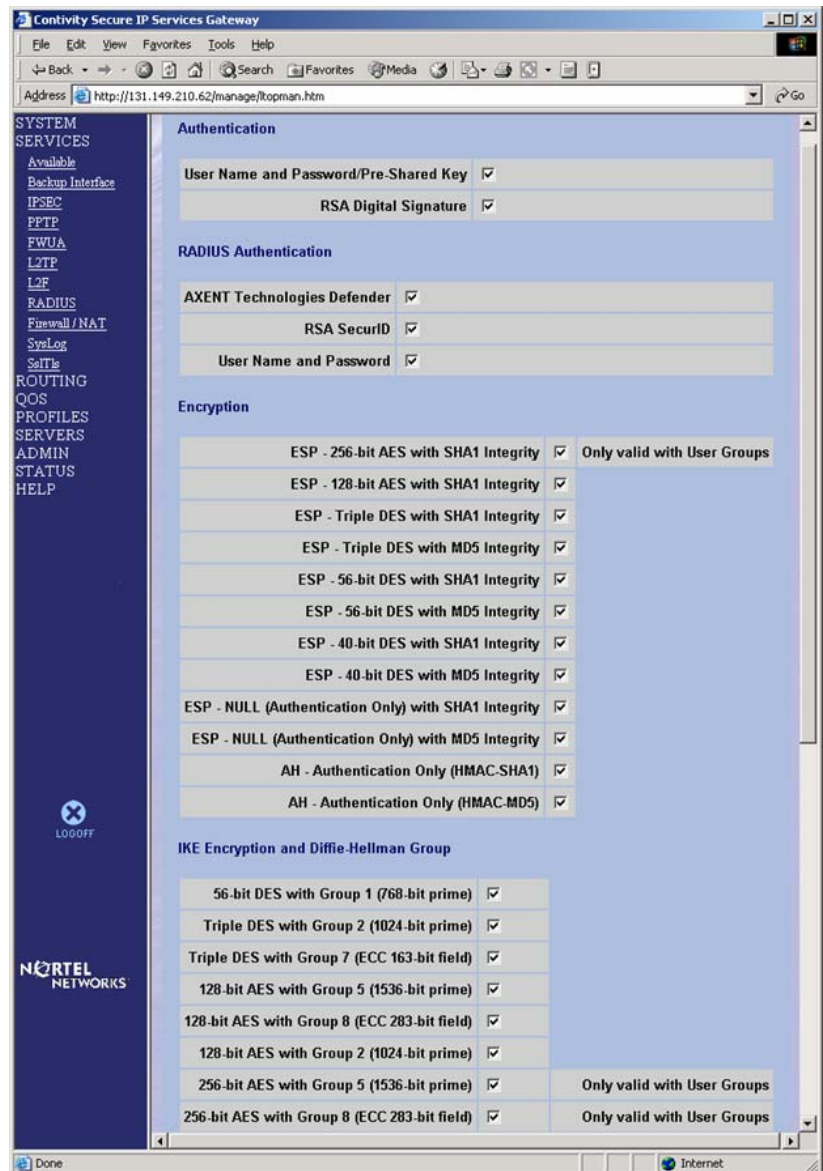
Use Procedure 7 to set IPsec global variables.

**Procedure 7**  
**Setting IPsec global variables**

- 1 In the Contivity Secure IP Services Gateway navigator, select **SERVERS > IPsec**.

The IPsec Global Variables window appears, as shown in Figure 15 on [page 38](#)

**Figure 15**  
**IPsec global variables**



- 2 Select all the options in the **Authentication, Encryption, and IKE Encryption and Diffie-Hellmann Group** sections.
- 3 Click **OK**.

---

**End of Procedure**

---

## WLAN Handset 2212 group definition

Use Procedure 8 to create a WLAN Handset 2212 group.

### Procedure 8

#### Defining a WLAN Handset 2212 group

- 1 In the Contivity Secure IP Services Gateway navigator, select **PROFILES > Groups**.

The Add Groups window appears, as shown in Figure 17 on [page 40](#)

**Figure 16**

**Add groups**



- 2 Click **Add**.
- 3 Enter a **Group Name** and select a **Parent Group**.

The Group details window appears, as shown in Figure 17 on [page 40](#).

**Figure 17**  
**Group details**



- 4 Click **Apply**.
- 5 Click **OK**.

---

End of Procedure

---

## WLAN Handset 2212 group IPsec variables

Use Procedure 9 to set IPsec variables for a WLAN Handset 2212 group.

### Procedure 9 Setting IPsec variables for a WLAN Handset 2212 group

- 1 In the Contivity Secure IP Services Gateway navigator, select **PROFILES > Groups**.

The Add Groups window appears, as shown in Figure 18 on [page 41](#).

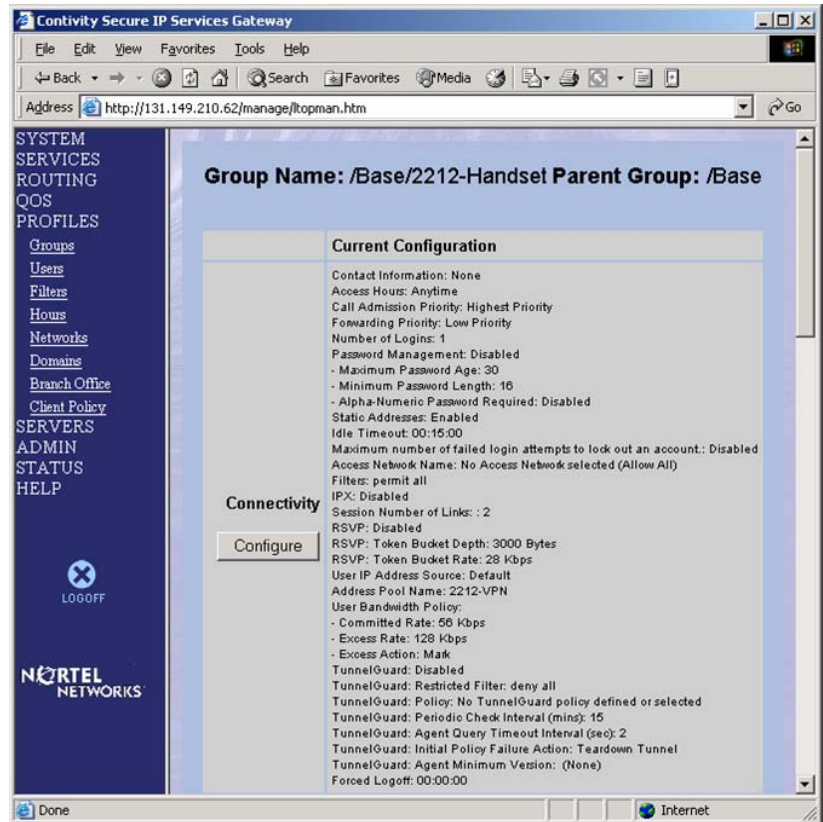
**Figure 18**  
**Add groups**



- 2 Click **Edit** next to the group for which you want to set the variables.

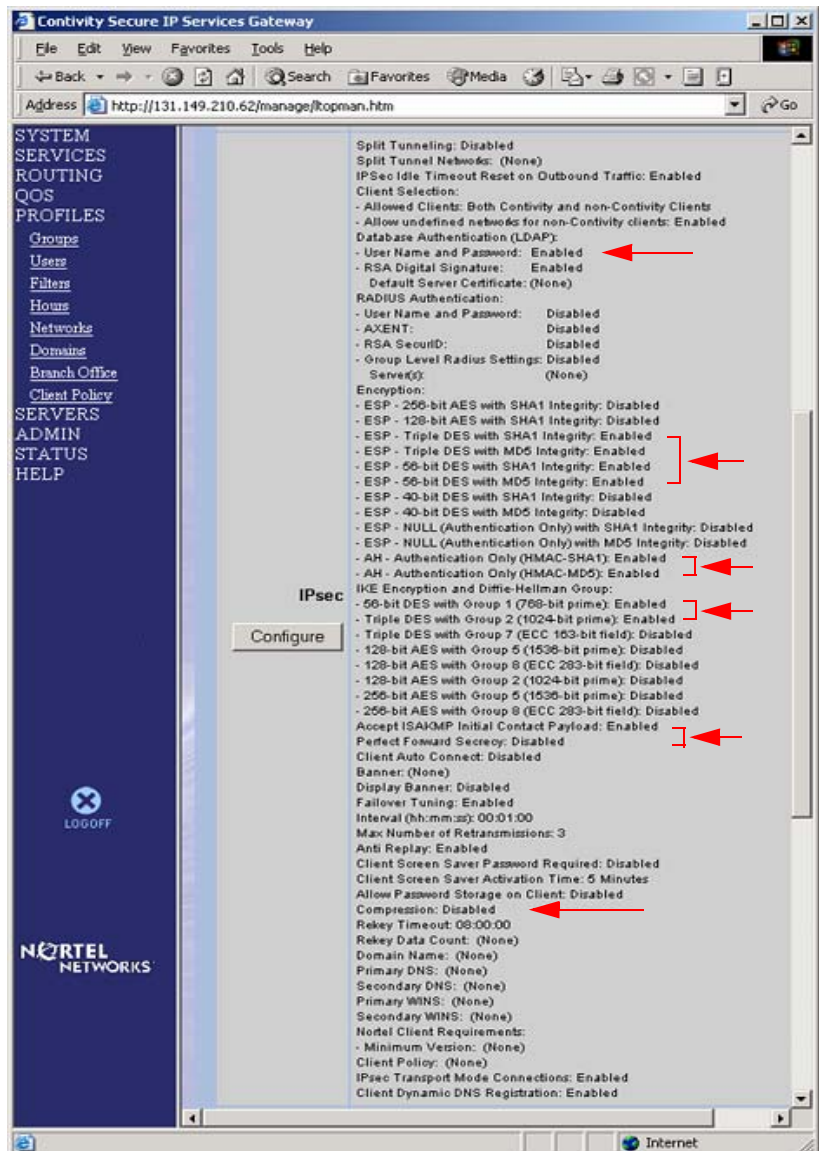
The IPsec Variables window appears. The Connectivity section is shown in Figure 19 on [page 42](#); the IPsec section is shown in Figure 20 on [page 43](#).

**Figure 19**  
**IPsec variables - Connectivity section**



- 3 Configure the Connectivity variables.
  - a. Click **Configure** in the **Connectivity** section.
  - b. If you intend to use the same unit, set **Number of Logins** to 1.
  - c. Enter an ID for the **Address Pool Name**.

**Figure 20**  
**IPsec variables - IPsec section**



- 4 Configure the IPsec variables.
  - a. Click **Configure** in the **IPsec** section.
  - b. Enable the following items (indicated by arrows in Figure 20 on [page 43](#)):
    - **User name and Password**
    - **ESP - Triple DES with SHA1 Integrity**
    - **ESP - Triple DES with MD5 Integrity**
    - **ESP - 56-bit DES with SHA1 Integrity**
    - **ESP - 56-bit DES with MD5 Integrity**
    - **AM - Authentication Only (HMAC-SHA1)**
    - **AM - Authentication Only (HMAC-MD5)**
    - **56-bit DES with Group 1 (768-bit prime)**
    - **Triple DES with Group 2 (1024-bit prime)**
    - **Accept ISAKMP Initial Contact Payload**
  - c. Disable the following (indicated by arrows in Figure 20 on [page 43](#)):
    - **Accept Forward Secrecy**
    - **Compression**

---

End of Procedure

---

---

# Users, interface and firewall configuration

---

## Contents

This section contains information on the following topics:

|                                                          |                    |
|----------------------------------------------------------|--------------------|
| <a href="#">Introduction . . . . .</a>                   | <a href="#">45</a> |
| <a href="#">User accounts . . . . .</a>                  | <a href="#">45</a> |
| <a href="#">Second interface configuration . . . . .</a> | <a href="#">48</a> |
| <a href="#">Firewall configuration . . . . .</a>         | <a href="#">52</a> |

## Introduction

This section describes how add user accounts, configure the second interface, and configure the firewall.

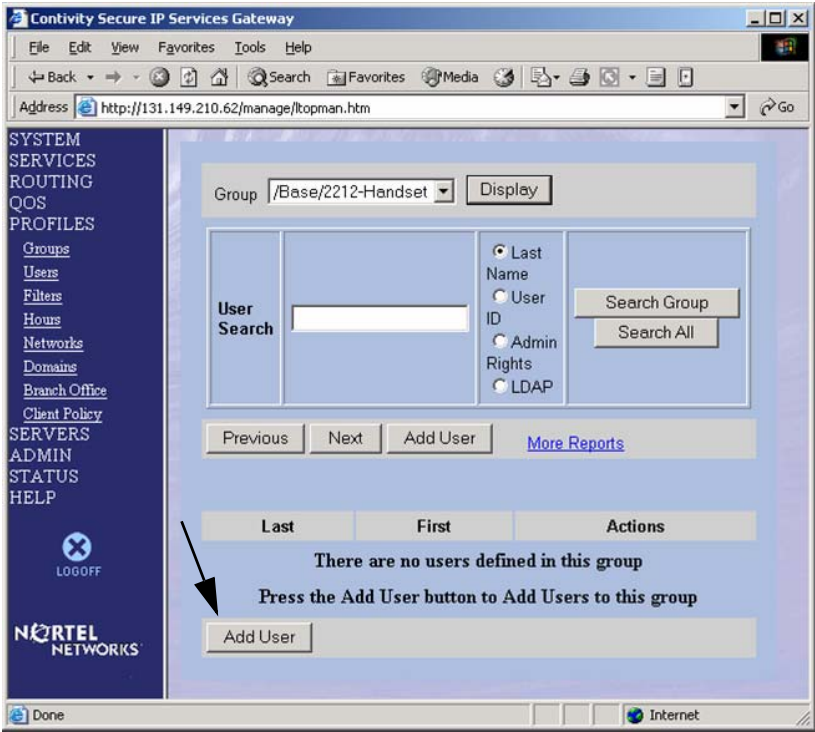
## User accounts

Use Procedure 10 to add a user account.

### Procedure 10 Adding a user account

- 1 In the Contivity Secure IP Services Gateway navigator, select **PROFILES > Users**.  
The Users window appears, as shown in Figure 21 on [page 46](#).

**Figure 21**  
**Adding users**



2 Click **Add User**, as indicated by the arrow.

The Users Details window appears, as shown in Figure 22 on [page 47](#)

**Figure 22**  
**User details**

The screenshot shows the 'Contivity Secure IP Services Gateway' web interface. The left sidebar contains a navigation menu with the following items: SYSTEM, SERVICES, ROUTING, QOS, PROFILES, Groups, Users, Filters, Hous, Networks, Domains, Branch Office, Client Policy, SERVERS, ADMIN, STATUS, and HELP. The main content area is divided into two sections: 'General' and 'User Accounts'.

**General Section:**

- Name:** Fields for 'First' (containing 'K.P.') and 'Last' (containing 'Rao').
- Group:** A dropdown menu showing '/Base/2212-Handset'.
- Static IP Address:** A text field.
- Static Subnet Mask:** A text field.
- Remote User:** A text field.
- Note:** 'The static IP subnet mask is used for IPsec connections only.'

**User Accounts Section:**

|                              | User ID | Password | Confirm Password | Expires (Days) | Status |
|------------------------------|---------|----------|------------------|----------------|--------|
| IPsec                        | krso    | AAAAA    | AAAAA            |                |        |
| PPTP                         |         |          |                  |                |        |
| L2TP                         |         |          |                  |                |        |
| L2F                          |         |          |                  |                |        |
| Firewall User Authentication |         |          |                  |                |        |

- 3 In the **General** section, enter a **First** and **Last** name.
- 4 Select the **Group** to which the user will belong.
- 5 In the **User Accounts** section, enter a **User ID** and **Password**.
- 6 Re-enter the password.
- 7 Click **OK**.

---

**End of Procedure**

---

## Second interface configuration

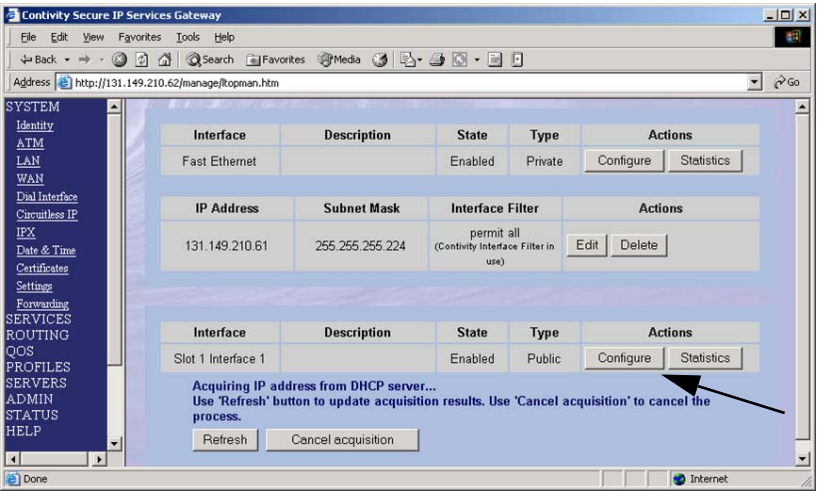
Use Procedure 11 to configure the second interface.

### Procedure 11 Configuring the second interface

- 1 In the Contivity Secure IP Services Gateway navigator, select **SYSTEM > Users**.

The Second Interface window appears, as shown in Figure 23.

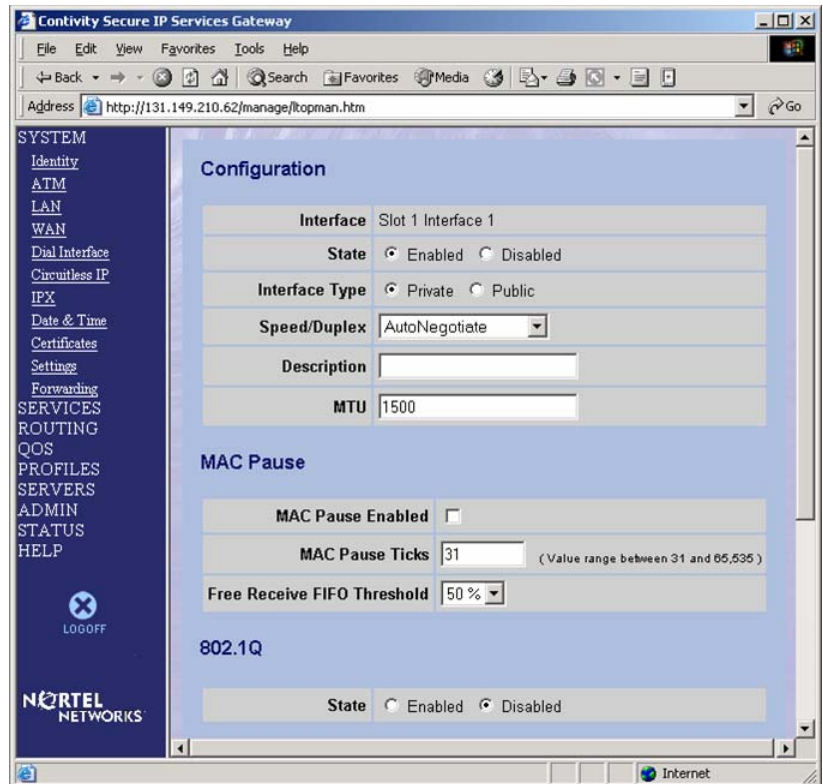
**Figure 23**  
Configuring second interface



- 2 Click **Configure** (as indicated by the arrow).

The Second Interface detail window appears, as shown in Figure 24 on [page 49](#).

**Figure 24**  
**Second interface details**



3 In the **Configuration** section, select **Private** for **Interface Type**.

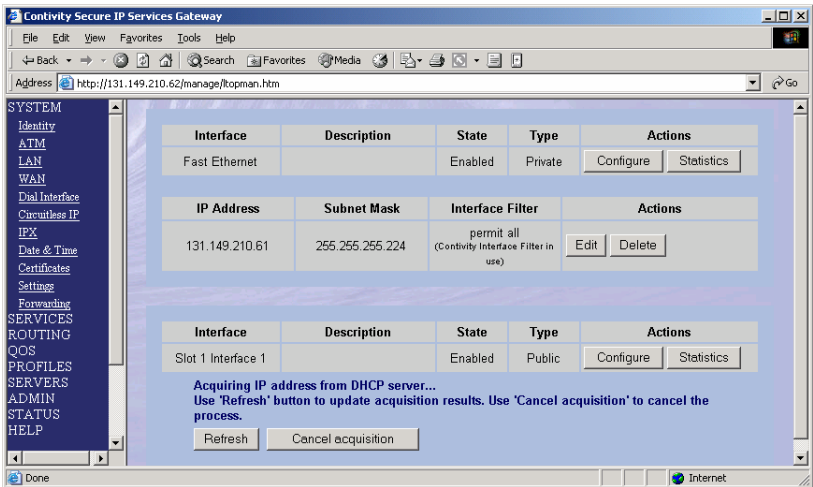
4 In the **802.1Q** section, select **Disabled** for **State**.

5 Reboot the computer for the settings to take effect.

**Note:** The need to reboot may depend on the router model as there may be a spare private interface on the model.

6 Once the computer has rebooted, reload the second interface window.

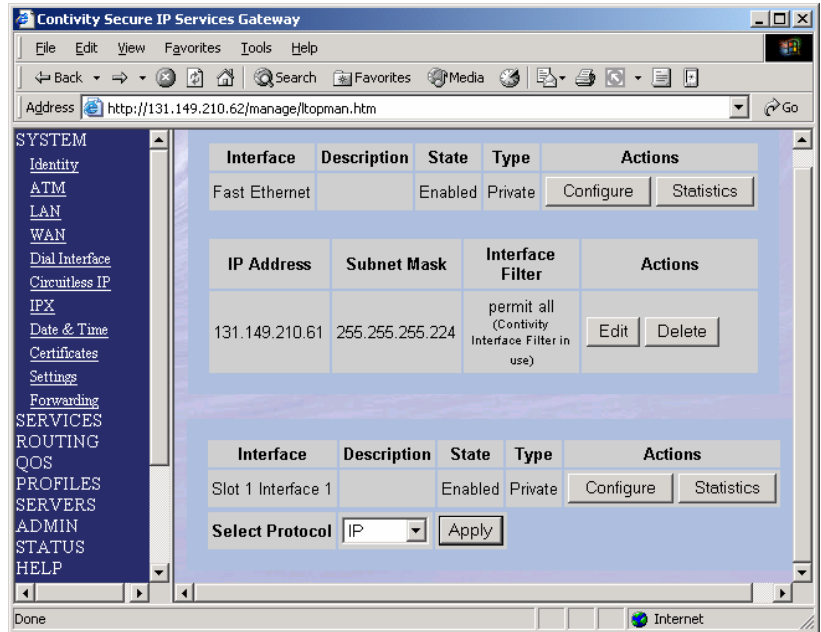
**Figure 25**  
**Cancel acquisition**



7 Click **Cancel acquisition**.

The Second Interface page reloads as shown in Figure 26 on [page 51](#).

**Figure 26**  
**Select protocol**



- 8** Select **IP** in the **Select Protocol** list.
- 9** Click **Apply**.

**End of Procedure**

## Firewall configuration

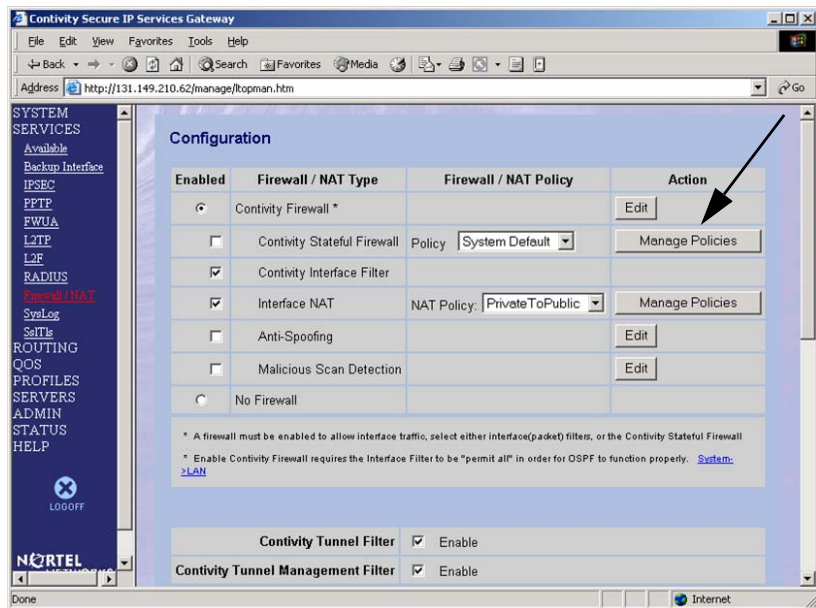
Use Procedure 12 configure the firewall.

### Procedure 12 Configuring the firewall

- 1 In the Contivity Secure IP Services Gateway navigator, select **SERVICES** > **Firewall/NAT**.

The Firewall Options window appears, as shown in Figure 27.

**Figure 27**  
**Firewall options**



- 2 Select **Contivity Firewall**.
- 3 Select **Contivity Stateful Firewall**.
- 4 Clear **Contivity Interface Filter**.
- 5 Clear **Interface NAT**.
- 6 Clear **Contivity Tunnel Filter**.

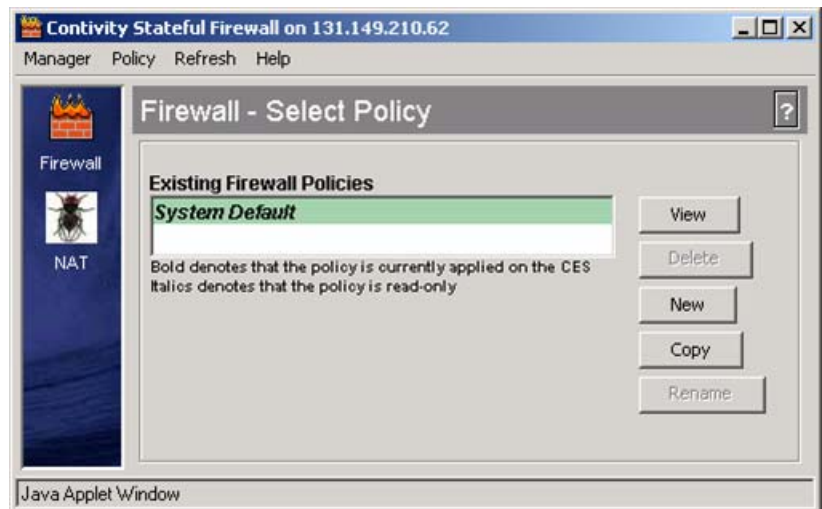
- 7 Click **OK**.

**Note:** Do not leave this step for later as mobile clients will be unable to get an IP address via DHCP.

- 8 After the wireless gateway has rebooted, click **Manage Policies** (as indicated by the arrow).
- 9 Enter the login and password you entered when you created the user account in "User accounts" on [page 45](#).

The Firewall Policies window appears, as shown in Figure 28.

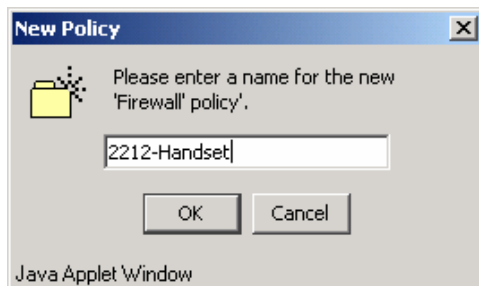
**Figure 28**  
**Firewall policies**



- 10 Click **New**.

The New Policy window appears, as shown in Figure 29 on [page 54](#)

**Figure 29**  
**New policy**



**11** Enter a name for the new firewall policy.

**12** Click **OK**.

The new policy is created and the Firewall Policy-Edit window appears, as shown in “Edit firewall policy” on [page 54](#).

**Figure 30**  
**Edit firewall policy**



**13** Select the **Override Rules** tab.

- 14 Right-click in the tab and select **Add New Rule**.

A set of default rules is created on the tab as shown in Figure 31.

**Figure 31**  
**Override Rules**

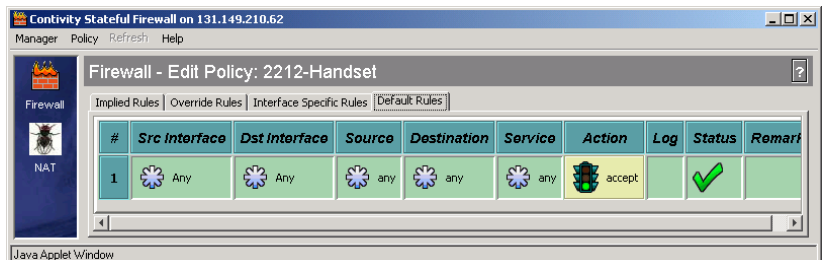


- 15 Select the **Default Rules** tab.

- 16 Right-click in the tab and select **Add New Rule**.

A set of default rules is created on the tab as shown in Figure 32

**Figure 32**  
**Default Rules**



- 17 Select **Manager > CSF/NAT**.

- 18 Click **Yes** to exit

- 19 Click **Yes** to save the changes, and return to the Firewall Options page.

- 20 Select the policy you created starting at step 11 from the **Policy** list in the **Firewall/NAT Policy** section.

**21** Click **OK**.

\_\_\_\_\_ **End of Procedure** \_\_\_\_\_

---

# Handset configuration

---

## Contents

This section contains information on the following topics:

|                                               |    |
|-----------------------------------------------|----|
| <a href="#">Introduction</a> .....            | 57 |
| <a href="#">Configuring the handset</a> ..... | 57 |

## Introduction

This section describes how to configure the WLAN Handset 2212.

## Configuring the handset

There are two ways to configure the WLAN Handset 2212:

- Using the configuration cradle  
This method is preferred for bulk configurations.
- Using the handset screen

### Configuration cradle method

Use Procedure 13 on [page 58](#) to configure the WLAN Handset 2212 using the cradle method.

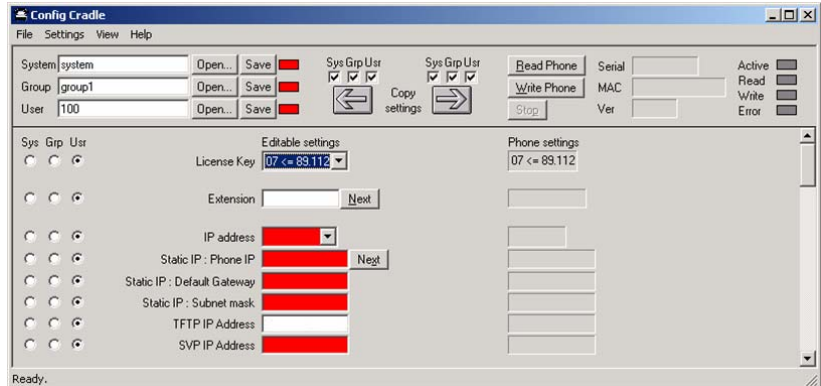
### Procedure 13

#### Configuring the WLAN Handset 2212 using the cradle

- 1 Before you begin, do the following:
  - a. Remove the battery before placing the handset in the cradle
  - b. Connect the serial cable to the COM port.
  - c. Load the latest software (0.60 or later) on the telephone. The configuration cradle only works with Phase II software (0.60 or later).
- 2 Decompress the configuration cradle file (version 2.11.02) to a folder on the hard drive.
- 3 Double-click on **PhoneConfig.exe** in the folder.

The Config Cradle window appears, as shown in Figure 33. The settings for the telephone are grouped into three main categories: System, Group, and User. User is the default group for the settings at startup and this should be sufficient for a few phones. For larger deployments, planning will be required for the settings.

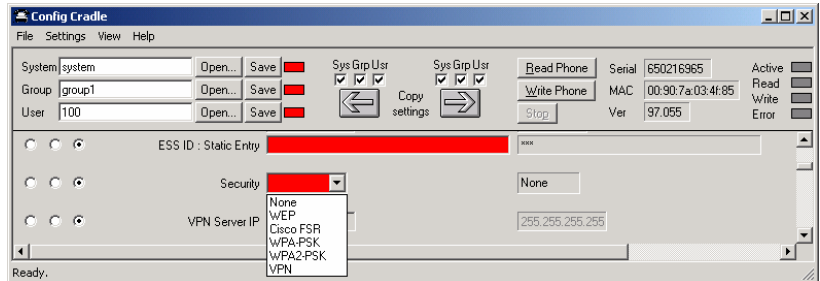
**Figure 33**  
**Config Cradle window**



- 4 Place the handset in the cradle.
- 5 Click **Read Phone** on the configuration tool.

The tool is populated with the VPN settings as shown in Figure 34 on [page 59](#).

**Figure 34**  
**Config Cradle with VPN Settings**



**6** Click **Save**.

**End of Procedure**

## Handset screen method

Use Procedure 14 to configure the WLAN Handset 2212 using the screen method.

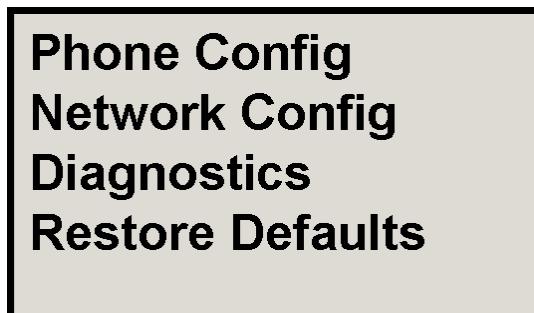
### Procedure 14

Configuring the WLAN Handset 2212 using the screen

- 1** Turn on the handset.
- 2** To access the Configuration menu, press the green key and red key simultaneously, then release the green key first.

The Configuration menu appears on the display, as shown in Figure 35 on [page 60](#).

**Figure 35**  
**Configuration menu**



- 3**    Set the Licence Option.
  - a.**    Select **Phone Config > License Option**.
  - b.**    Enter **010** using the keypad on the handset.
  - c.**    Select **Save**.
- 4**    Set the Terminal Type.
  - a.**    Select **Phone Config > License Option**.
  - b.**    Select **i2004**.
  - c.**    Select **Save**.
- 5**    Set the DHCP IP address.
  - a.**    Select **Network Config > IP Addresses > Use DHCP**.
  - b.**    Select **OK**.
- 6**    Set the VPN Server IP address.
  - a.**    Select **Network Config > Security > Static Entry > VPN > VPN Server IP**.
  - b.**    Enter **010.010.010.011**.
  - c.**    Select **OK**.
- 7**    Set Mode.
  - a.**    Select **Network Config > Security > Static Entry > VPN > VPN Client IP > IKE Mode Config > Phase 1 - ISAKMP**.

- b. Set **Mode** to **Aggressive**.
  - c. Select **OK**.
- 8 Set your password.
  - a. Select **Network Config > Security > Static Entry > VPN > VPN Client IP > IKE Mode Config > Phase 1 - ISAKMP > Preshared Key > Alphanumeric**.
  - b. Enter your password.
  - c. Select **Save**.
- 9 Set the Phase 1 authentication parameters.
  - a. Select **Network Config > Security > Static Entry > VPN > VPN Client IP > IKE Mode Config > Phase 1 - ISAKMP**.
  - b. Select **Diffie-Hellman > Group 1**.
  - c. Select **OK**.
  - d. Select **Auth. Hash > SHA1**.
  - e. Click **OK**.
  - f. Select **Encryption > 3DES**.
  - g. Click **OK**.
- 10 Set Key ID.
  - a. Select **Network Config > Security > Static Entry > VPN > VPN Client IP > IKE Mode Config > Phase 1 - ISAKMP > Local ID > Key ID**.
  - b. Enter the key ID.
  - c. Click **Save**.
- 11 Set Phase 1 Lifetime.
  - a. Select **Network Config > Security > Static Entry > VPN > VPN Client IP > IKE Mode Config > Phase 1 - ISAKMP > Lifetime (sec)**.
  - b. Enter **2678400**.
  - c. Click **Save**.
- 12 Set Phase 1 Options.
  - a. Select **Network Config > Security > Static Entry > VPN > VPN Client IP > IKE Mode Config > Phase 1 - ISAKMP > Options**.

- b. Select **Init Contact**.
  - c. Click **OK**.
  - d. Select **Nortel features**.
  - e. Click **OK**.
- 13 Set the Phase 2 authentication parameters.
  - a. Select **Network Config > Security > Static Entry > VPN > VPN Client IP > IKE Mode Config > Phase 2 - ESP**.
  - b. Select **Auth. Hash > SHA1**.
  - c. Click **OK**.
  - d. Select **Encryption > 3DES**.
  - e. Click **OK**.
- 14 Set IP address and subnet.
  - a. Select **Network Config > Security > Static Entry > VPN > VPN Client IP > IKE Mode Config > Phase 2 - ESP > Remote Network**.
  - b. Select **IP Address**.
  - c. Set the IP address to that of the VPN router.
  - d. Click **Save**.
  - e. Select **IP Subnet**.
  - f. Set the IP subnet to that of the VPN router.
  - g. Click **Save**.
- 15 Set Phase 2 Lifetime.
  - a. Select **Network Config > Security > Static Entry > VPN > VPN Client IP > IKE Mode Config > Phase 2 - ESP > Lifetime (sec)**.
  - b. Enter **2678400**.
  - c. Click **Save**.

---

End of Procedure

---



Nortel Communication Server 1000

## **WLAN Handset 2212**

### Installation and Configuration for VPN

Copyright © Nortel Networks Limited 2005  
All Rights Reserved

Information is subject to change without notice.  
Nortel Networks reserves the right to make changes in design  
or components as progress in engineering and manufacturing  
may warrant.

Nortel, Nortel (Logo), the Globemark, This is the Way, This is  
Nortel (Design mark), SL-1, Meridian 1, and Succession are  
trademarks of Nortel Networks.

Publication number: 553-3001-229  
Document release: Standard 1.00  
Date: November 2005  
Produced in Canada



>THIS IS **THE WAY**

>THIS IS **NORTEL™**